NetCyber Team 3 Hackathon: Securing a Local Server on a VM

This presentation explores best practices for setting up and securing a local server on a virtual machine (VM) while ensuring accessibility and maintaining strong security measures.

Intro: Importance of Server Setup and Security

Canva

NetCyber Hackathon Step-By-Step Hackathon

1

Data Protection

Secure server setup is vital for safeguarding sensitive data from unauthorized access and cyber threats.

2

System Reliability

A well-configured server ensures stable operation and minimizes downtime, crucial for business continuity.

3

Scalability and Efficiency

A well-planned server setup supports business growth by accommodating increased traffic and user demand without performance degradation.

4

Compliance

Meeting industry standards and regulations requires secure server practices to protect sensitive information.

VM Fundamentals: Advantages and Considerations

Advantages

Virtualization offers flexibility, cost-effectiveness, and resource optimization.

- Resource sharing
- Easy deployment
- Scalability

Considerations

Choose the right VM platform and configure security settings for optimal performance and security.

- VM security
- Performance impact
- Resource allocation

VM Security

Virtual machines introduce specific security concerns that need to be addressed.

- VM escape vulnerabilities
- Hypervisor security
- Guest OS hardening

Tools Used:
Installing and Configuring the Local Server

1. ### Select a Server OS

   Chose Virtual Machine Using ***Oracle VirtualBox***

2. ### Install the OS

   Use the chosen OS installer to set up the server on the VM.

3. ### Configure Initial Settings

   Configure basic settings like network, firewall, and user accounts.

4. ### Install Required Software

   Using ***Samba*** to create the folder sharing sytem and install essential software like databases, web servers, and security tools.

5. ### Test and Optimize

   Thoroughly test the server setup and optimize performance for optimal efficiency by **pinging IP** and connecting to the ***network through the IP and shared folder***.

Network Configuration: Ensuring Accessibility

1

Define Network Interfaces

Configure network interfaces for the VM to allow access to the server.

2

Assign IP Address

Assign a static or dynamic IP address to the server for reliable communication.

Ours is dynamic so it changes today

3

Configure DNS

Set up DNS entries to resolve the server's domain name to its IP address.

4

Firewall Rules

Configure firewall rules to allow incoming and outgoing traffic based on the server's function.

Set up using command ***ufw*** as the root user.

Allow samba through the firewall as well. Check the status for allowability should say samba is allowed.

5

Test Connectivity

Test network connectivity from different devices to ensure accessibility.

Via pinging the IP and by checking via entering the shared folder and logging in.

Best Practices for Server Security

Strong Passwords

Use complex passwords for all user accounts and enable authentication.

Using ***apt install libpam-pwquality***

Regular Updates

Keep the server operating system, software, and security tools updated with the latest patches.

Using ***apt update/upgrade***

Secure Server Configuration

- **Minimal Installations**: Install only essential software and services to reduce attack surfaces.
- **Default Settings**: Change default passwords, ports, and configurations.
- **Disable Unused Features**: Turn off unnecessary services, network interfaces, and protocols.

Firewall and Access Controls

Firewall	Access Controls
A barrier that filters network traffic.	Restricting user access to specific resources and functions.
Prevents unauthorized access to the server.	Ensures only authorized personnel have access to sensitive information.
Configured to block or allow specific connections.	Utilize user roles and permissions to grant access based on job responsibilities.

Team Breakdown

1

Production Team

Jordan, Keira, and Elvin handle the operational aspects of the hackathon, including server setup and configuration.

2

Research Team

Mahmud and Shakeel are responsible for researching security best practices and vulnerabilities.

3

Collaboration

Both teams work together to ensure the server is secure and that the hackathon runs smoothly.

Monitoring and Powering Off

1

System Performance

- **CPU Usage:**
  Check for high usage processes to avoid slowdowns. Use tools like `top` or Task Manager.
- **Memory Usage:**
  Monitor RAM to prevent system crashes. Tools: `htop` or Resource Monitor.
- **Disk Activity:**
  Track read/write speeds to spot issues. Tools: `iostat` or Disk Management.
- **Network Activity:**
  Watch bandwidth usage for unusual traffic. Tools: `iftop` or Network Monitor.

2

Powering off

- **Safe Shutdown:**
  Always shut down properly to prevent data loss. Examples:
- Linux: `sudo shutdown now`
- Windows: Start → Shut Down.
- **Force Shutdown:**
  Use the power button only if the system is stuck.
- **Scheduled Shutdown:**
  Automate shutdowns to save energy. Example: `shutdown -h +60` (Linux).